PGP® Desktop Version 9.9 for Mac OS X Release Notes

Thank you for using this PGP Corporation product. These Release Notes contain important information regarding this release of PGP Desktop for Mac OS X. PGP Corporation strongly recommends you read this entire document.

PGP Corporation welcomes your comments and suggestions. Please use the information provided in Getting Assistance to contact us.

Product: PGP Desktop for Mac OS X

Version: 9.9.0

Warning: Export of this software may be restricted by the U.S. government.

Note: To view the most recent version of this document, please go to the PGP Support Portal and view the Knowledge Base article *PGP User Guides, Administrator Guides, Quick Start Guides, and Release Notes* (https://support.pgp.com/?faq=589).

What's Included in This File

- About PGP Desktop
- Changes in this release
- System Requirements
- Installation Instructions
- Licensing
- Additional Information
- Getting Assistance
- Copyright and Trademarks

About PGP Desktop for Mac OS X

PGP Desktop is a security tool that uses cryptography to protect your data against unauthorized access.

Changes in This Release

This section lists the changes and new features in this release of PGP Desktop.

What's New in PGP Desktop for Mac OS X Version 9.9

Building on PGP Corporation's proven technology, PGP Desktop 9.9 for Mac OS X includes numerous improvements and the following new features.

General

- **User Interface Modifications for ADA Compliance.** Compliance with the Americans with Disabilities Act (ADA) standards for accessible design continues to improve in this release. PGP Universal Server now provides keyboard equivalents for all actions in PGP Universal Web Messenger and PGP Verified Directory web pages. The PDF documentation for all PGP products in this release is tagged to facilitate reading and navigation of the documentation by users of assistive technology.

PGP Whole Disk Encryption

- **Enhanced PGP WDE Policy.** Administrators now have fine-grained control of end-user PGP Whole Disk Encryption permissions. For example, an Administrator can now manage boot disk functions separately from removable disk functions by preventing the decryption of boot disks, while allowing the encryption and decryption of removable disks.
- **PGP WDE Boot Drive Support for Mac OS X.** Encryption of the boot drive is now available on Intel-enabled Mac OS X 10.4 and 10.5 systems. The software can be managed by PGP Universal Server, supporting standard PGP WDE WDRT functionality, logging and reporting, and identification of Mac OS X platforms within PGP Universal Server, permitting the administrator to identify whether a device is a Windows or Mac OS X platform. This feature is not compatible with Boot Camp software.

PGP Messaging

- **Offline Policy controls.** Administrators can now enforce policy for offline users by controlling what happens to email when the PGP Universal Server cannot be reached by PGP Desktop. Options include blocking outbound messages, sending outbound messages in the clear, or allowing users to follow locally defined policy. A PGP Notifier-like window can optionally be presented, informing the user that policy could not be executed, and asking if the user would like to send the message unsecured. Any use of client offline bypass is logged to PGP Universal Server.

PGP Universal Server Logging

- **Rich Client Policy Logging.** PGP Universal Server now logs a variety of information about the client's receipt and use of downloaded policy. This information also includes the list of enabled PGP Desktop modules, license information for the client, and PGP NetShare folder encryption processing preferences (that is, specified white lists and black lists for the client).
- **Enhanced Centralized Event Logging.** PGP Universal Server provides expanded reporting on PGP Whole Disk Encryption usage on client systems. Information now provided includes the user name and primary email address associated with the system, the last access by the user, the version of PGP Desktop in use, and other system-specific information.

Resolved Issues

For a list of issues that have been resolved in this release, please go to the PGP Support Portal and view Knowledge Base Article 1014 (https://support.pgp.com/?faq=1014).

System Requirements

- Apple Mac OS X 10.4.x, 10.5.x (Intel or PowerPC)
- 512 MB of RAM
- 64 MB hard disk space

Note: To encrypt your Mac OS X boot disk with PGP Desktop 9.9 you must be using Mac OS X version 10.4.10 or later on Intel-based Macintosh systems only.

Compatible Email Client Software

PGP Desktop will, in most cases, work without problems with any Internet-standards-based email client that runs on Mac OS X 10.4.x or Mac OS X 10.5.x.

- Apple Mail 2.1.1, 3.3
- Microsoft Entourage 2008

Note: A new PGP Mail Plugin is available for computers running Mac OS X version 10.5.6. This plugin is available from the PGP Corporation Knowledgebase article #1099 (https://support.pgp.com/?faq=1099). Older versions of Mac OS X are still compatible with the PGP Mail Plugin included with PGP Desktop.

Instant Messaging Client Compatibility

PGP Desktop is compatible with the following instant messaging clients when encrypting AIM instant messages, file transfers, and direct connections:

- iChat 3.1.x, 4.0

  Encryption of file transfers and direct connections requires AIM 5.9.3702 on Windows or iChat 3.1 on Mac OS X. Audio and video connections are not encrypted by PGP Desktop.

Other instant messaging clients may work for basic instant messaging, but have not been certified for use.

Anti-Virus Client Software Compatibility for Macintosh

- **Norton Antivirus 11 and Norton Internet Security 3.0**: To use PGP Desktop with email and instant messaging, you must disable the Vulnerability Protection option in Norton. To do this, select Auto Protection and then disable the option for Vulnerability Protection." [18130]

Installation Instructions

To install PGP Desktop on your Mac OS X system:

1. Mount the PGP Desktop disk image.
2. Double-click `PGP.pkg`.
3. Follow the on-screen instructions.

Licensing

PGP Desktop uses a licensing system to determine what features will be active. You enter your PGP Desktop license using the Setup Assistant after installation. If you are in a domain protected by a PGP Universal Server, your PGP administrator may have configured your PGP Desktop installer with a license.

You can also use PGP Desktop without a license, but for non-commercial use only. Commercial use of PGP Desktop without a license is a violation of the End-User License Agreement (EULA). If you choose to use PGP Desktop without a license (and you are legally permitted to do so under the EULA for non-commercial use), most PGP Desktop features will not work; only basic functionality will be available.

For more information about PGP Desktop licensing and purchase options, go to the PGP Store (https://store.pgp.com/).

Additional Information

General

- **Installation:** This version of PGP Desktop replaces all older PGP products, as well as replacing PGP Universal Satellite 2.X. These products will be removed as part of upgrading to PGP Desktop. [NBN]

PGP Whole Disk Encryption

- **Encrypting Book Disks for Intel-based Macintoshes:** PGP Desktop 9.9 for Mac OS X supports encrypting boot disks for Intel-based Macintoshes. PGP Desktop 9.9 for Mac OS X installs and works perfectly on PowerPC-based Macintoshes, but you cannot use the PGP WDE feature to encrypt the boot disk. [NBN]

  Note: To encrypt your Mac OS X boot disk with PGP Desktop 9.9 you must be using Mac OS X version 10.4.10 or later.

- **Safe Boot**: The Mac OS X Safe Boot feature does not work on a boot disk that has been whole disk encrypted; Safe Boot disables kernel extensions required by PGP WDE. If you hold down the Shift key after authenticating at the PGP BootGuard screen, the system will *not* boot; however, it does restart after a few minutes. [17770]
- **Boot Camp**: Apple Boot Camp is **not** compatible with PGP Desktop 9.9 for Mac OS X. You **must** uninstall Boot Camp from a system *before* you install PGP Desktop. Do not add Boot Camp to a system on which PGP Desktop 9.9 for Mac OS X is installed; it will not work. Other virtualization software (Parallels Desktop for Mac, for example) works normally with PGP Desktop 9.9 for Mac OS X. [15433, 17399] (
- **PGP WDE and Recovery Applications**: Be sure you decrypt your disk before you run any disk recovery applications (such as DiskWarrior from Alsoft). [18157]
- **Previously Encrypted Partitions or Disks:** If you used the PGP Whole Disk Encryption feature of previous versions of PGP Desktop for Mac OS X, you **must** decrypt those non-boot partitions or disks (including USB flash drives) *before* installing Version 9.9 or you will no longer be able to access the data on them. You can re-encrypt the partitions/disks with PGP Desktop 9.9 for Mac OS X once it is installed. [NBN]
- **Modifying the system partition:** Do not make any changes to the system partition on a boot disk that has been encrypted by PGP WDE; it will fail to boot properly on the next startup. If you must make changes to the partitioning of an encrypted disk, *decrypt the disk first* and then make the partition changes.
- **Supported passphrase characters**: The following characters are supported:

  `abcdefghijklmnopqrstuvwxyz`

  `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

  `0123456789`

  `` `!@#$%^&*()_+={}\\|:;[]'\"<>,.?/- ``

  Any other characters, including accented characters (such as `ç é è ê ë î ï ô û ù ü ÿ`) or symbols (such as `¢ ® œ`), are not supported. [12947, 11551, 18871]

  Apple JIS keyboards are not allowed `` ` `` or ~
- **Using Apple JIS Keyboards**: When using the Apple JIS keyboard with PGP WDE 9.9.0 on Mac OS X for boot disk encryption, the keyboard layout at boot time is always US English layout although it is Japanese layout when you create a passphrase before encrypting your drive. The following keys are re-mapped on your keyboard:

  ~`@^&*()-_=+|{}[]"':

  If you are unable to change your keyboard layout within Mac OS X when encrypting your drive and you use these keys in your passphrase, please be aware you may need to type different keys than normal to locate the re-mapped key on your keyboard layout. [18140]
- **Reformatting an HFS Partition**: Reformatting an HFS partition on an MBR disk results in all partitions of the disk being erased (rather than the one specified). This can result in unintentional loss of data. This applies only if PGP WDE is installed. [12437]
- **Hibernation:** PGP Whole Disk Encryption no longer disables Safe Sleep automatically as it is not installed by default. If you insert removable disks protected by PGP WDE during boot time on a system configured to use Safe Sleep, you may experience problems sleeping the machine. We recommend disabling Safe Sleep in such circumstances. Run the `sudo pmset -a hibernatemode 0` command from Terminal to disable Safe Sleep. [11320]
- **Secondary partitions:** Secondary APM partitions physically located on your boot volume are not available for encryption on Intel-based Mac OS X machines. GPT formatted partitions are supported. [11025]
- **PGP WDE and NitroAV PCMCIA/Firewire 800 Adaptors:** Removable devices connected to a MacBook Pro using a NitroAV PCMCIA/Firewire 800 adapter are not currently supported. [11936]

PGP Messaging

- **Thunderbird Email Sent to BlackBerry Users**: If your Thunderbird email client is set to send email in HTML-only format, and the message is encrypted by either PGP Universal Server or PGP Desktop before it arrives at the BES gateway, the recipient will be unable to view the email message on his or

her BlackBerry. To work around this issue, configure your Thunderbird email client so that it does not send HTML-only messages. [16273]

- **Adding comments to secured messages:** To ensure proper display of comments added to secured messages per the **Add a comment to secured messages** option, PGP Corporation recommends using ASCII text in the Comment field. [11127]
- **S/MIME-signed email messages:** PGP may not process S/MIME signed emails if the signing X.509 certificate is not included in the email. The certificate is almost always included with the email unless the sender turns off this option. [9489, 9491]
- **Automatic mode:** PGP Desktop is initially installed in Automatic mode. You may change this in the Preferences if necessary to accommodate your environment. Automatic mode uses Mac OS X's built-in firewall functionality to redirect your email client connections through PGP Desktop. Some less common configurations may need to use Manual mode instead. If you fall into the categories below, you should switch to Manual mode in the PGP Preferences **(Messaging > Proxy Options > Email**). [NBN]

  These include:

  - Those with a requirement to use the built-in firewall for other purposes. Note that third-party applications can be installed to provide much more complete configuration options than the built-in user interface in System Preferences. These other solutions are compatible with PGP Desktop. Note that Norton Internet Security 3.0 does not use these methods, and is not compatible with Automatic mode.
  - Those who already redirect their email connections through, for instance, an SSH tunnel or VPN connection. Some VPN connections may cause problems with the connection diversion capabilities of PGP Desktop.
  - Automatic mode should *not* be used on a system which is also a mail server; use Manual mode instead.
- **Multiple users and Automatic mode:** If you fast user switch between multiple PGP Desktop users on a single Mac OS X machine, the first user to enable Automatic mode in PGP Desktop will be the only user who will be able to use Automatic mode; all other users must use Manual mode. If there are three or more users, each Manual mode user must bind to unique ports. [3335]
- **AOL Mail 10.3.7:** AOL Mail 10.3.7 is compatible only if you disable the PGP AIM proxy. To work around this issue, quit PGP engine (option-click PGP menu) before running AOL or configure PGP to use manual proxy mode instead of automatic. (Click Messaging, click Proxy Options, and then select Manual Proxy.) [12057]
- **Instant Messaging**: Encrypted file transfers fail on Intel Macintosh systems when the intended recipient is using a .Mac account. This applies only for file transfers sent to a .Mac recipient and only if both sender and recipient are using an Intel-based Macintosh. [13190]

PGP Shred

- **Shredding symbolic links:** Shredding symbolic links on the Mac will shred the linked file or directory. [8922]

Getting Assistance

Contacting Technical Support

- To learn about PGP support options and how to contact PGP Technical Support, please visit the PGP Corporation Support Home Page (http://www.pgp.com/support).
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit PGP Support Portal Web Site (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request Technical Support.**
- For any other contacts at PGP Corporation, please visit the PGP Contacts Page (http://www.pgp.com/company/contact/index.html).
- For general information about PGP Corporation, please visit the PGP Web Site (http://www.pgp.com).

- To access the PGP Support forums, please visit PGP Support (http://forum.pgp.com). These are user community support forums hosted by PGP Corporation.

Available Documentation

Prior to installation, complete Product Documentation is available through the PGP Support Knowledge Base (https://support.pgp.com/?faq=589).

PGP Desktop documentation is located in the Documentation folder on the disk image from which PGP Desktop is installed. All documents are saved as Adobe Acrobat Portable Document Format (PDF) files. You can view and print these files with Adobe Acrobat Reader, available at the Adobe Web site (http://www.adobe.com).

This release also includes online help in Apple Help format.

Copyright and Trademarks

Copyright © 1991-2008 PGP Corporation. All Rights Reserved. “PGP”, “Pretty Good Privacy”, and the PGP logo are registered trademarks of PGP Corporation in the U.S. and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.